UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	No. 14-CR-122 (CEJ)
DAVID SHEN,	)	
	)	
Defendant.	)	

GOVERNMENT'S TRIAL BRIEF AND
MOTION FOR PRE TRIAL ADMISSIBILITY OF EVIDENCE

COMES NOW the United States of America, by and through its attorneys, Richard G. Callahan, United States Attorney for the Eastern District of Missouri, and Gwendolyn E .Carroll, Assistant United States Attorney for said District, and submits the following trial brief.

I. Procedural History

On April 23, 2014, a Federal Grand Jury returned a three-count indictment against the defendant, David Shen, charging him with one count of Accessing a Protected Computer Without Authorization, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(i)-(iii) and 2, one count of Attempting to Access a Protected Computer Without Authorization, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(b) and 1030(c)(2)(B)(i)-(iii), and one count of Wire Fraud, in violation of 18 U.S.C. §§ 1343 and 2. On February 23, the defendant filed a Motion to Dismiss Counts 1 and 2 of the Indictment. ECF Doc. No. 30. The government opposed this motion, and on March 25, 2015, the parties appeared for a hearing on the motion. Doc. No. 35. At that time, the defendant withdrew his motion regarding Count 2. *Id.* On April 21, 2015, Judge Nannette Baker issued a Report and Recommendation recommending that the defendant's motion to dismiss

Count 1 be denied. Doc. No. 36. On May 21, 2015, the defendant filed an objection to the Report and Recommendation, and on May 26, 2015, this Court adopted the Report and Recommendation of the Magistrate Judge. Doc. Nos. 45, 47. This matter is set for trial to commence on June 22, 2015. Doc. No. 37.

II. Overview of the Facts

The government anticipates the evidence at trial will establish the following:

Defendant David Shen has a background in finance, as well as a master's degree in engineering. From around February 2009 until October 6, 2011, the defendant was employed as a "Manager of Asset Allocation & Risk Management" for Washington University Investment Management Company ("WU"). Generally speaking, the defendant worked on the WU endowment.

In late September 2011, the defendant learned that his direct supervisor (Brian Wentworth) was looking for a new job. In particular, there was a shared "Bloomberg" terminal at WU that WUIMC employees could access to consult the Bloomberg financial program. The defendant accessed the Bloomberg terminal when Wentworth had not logged out of his account, enabling the defendant to review some of Wentworth's correspondence. The defendant used a private e-mail account to "anonymously" send this information to Kim Walker ("Walker"), the Chief Investment Officer at WU. A brief investigation followed. Walker interviewed the defendant, who initially denied having sent the information regarding Wentworth. The defendant eventually admitted that he lied about sending the information. On October 6, 2011, Walker permitted the defendant to resign in lieu of termination, and he was subsequently escorted off the WU premises by security.

As part of his duties at WU, the defendant had been given password-protected access to various systems and databases, including third-party databases. These databases contain highly

confidential documents relating to the investments of the WU endowment. One of the third-party database systems belonged to a business known as Burgiss (referred to in the Indictment as "Service Provider B"). Another third-party system belonged to a business known as Albourne (referred to in the Indictment as "Service Provider A"). Washington University pays $400,000 per year for access to the Albourne service, and from October of 2008 until May of 2013, had paid Burgiss over $300,000 for its services. When the defendant resigned in lieu of termination, WU took steps to remove the defendant's access to computer systems, including third-party systems. There were four different Burgiss database accounts, and although the defendant's access to three of the four was successfully terminated, due to an oversight by Burgiss, the defendant's access to the fourth database was not cut off. Similarly, the defendant's access to the Albourne service was not shut down promptly upon the defendant's termination as a result of an oversight.

On November 22, 2011, over two months after the date of his resignation, the defendant called the Burgiss service requesting to have his password "unlocked." Burgiss notified WU, who then reviewed the defendant's access to the Albourne database, and discovered it had not been terminated. Between October 7, 2011 and November 23, 2011, the defendant had accessed Burgiss database records approximately seventeen times, downloading numerous documents and folders. According to WU, in the nine months prior, the defendant had accessed this database for work only about twelve times.

The defendant also accessed the Albourne database several times between October 6, 2011 and November 26, 2011. Following his resignation, the defendant downloaded approximately 800 documents from the Albourne and Burgiss databases, documents which he no longer had any legitimate business reason or justification to access.

II. Legal Issues

A. Elements of the Offense of Accessing a Protected Computer

Count One of the indictment charges the defendant with Accessing a Protected Computer Without Authorization, in violation of 18 U.S.C. § 1030(a)(2)(C). The essential elements of a violation of 18 U.S.C. § 1030(a)(2)(C) are:

(1) One, the defendant David Shen intentionally accessed a computer without authorization and

(2) Two, the defendant obtained information from any protected computer.

If the jury finds these two elements have been proven beyond a reasonable doubt, in order to trigger the felony provisions of 18 U.S.C. § 1030(c)(2)(B)(i) & (iii), the jury must then unanimously find that the answer to one of the following three questions is "yes":

(1) Did the defendant act for purposes of commercial advantage or private financial gain?

(2) Did the defendant obtain information that had a value exceeding $5,000.00?

If the jury finds that the answer to either of these two questions is "yes," then the felony provisions of 18 U.S.C. § 1030(c)(2)(B)(i) & (iii) have been satisfied.

Regarding the factor identified in § 1030(c)(2)(B)(ii) – that the defendant acted in furtherance of a crime or tort – although the government alleged that factor in the indictment in charging the provisions of the statute in the conjunctive, it does not intend to proceed on it as a theory at trial.[1]

1 "It is well established that where a statute may be violated by multiple means, the government may charge the statutory alternatives in the conjunctive (using the word 'and'). In other words, where the statute says 'or' the indictment should be pleaded as 'and' and may be proven as 'or.'" Federal Grand Jury Practice § 11.15. *United States v. Haymes*, 610 F.2d 309 (5th Cir. 1980). To avoid uncertainty in charging an offense in which the statute enumerates several different acts in the alternative, the preferred practice is to plead the offense by substituting the conjunction "and" for the disjunctive "or."

> When a statute specifies several alternative ways in which an offense may be committed, the indictment may allege the several ways in the conjunctive, and

B. Elements of the Offense of Attempting to Access a Protected Computer

Count Two of the indictment charges the defendant with Attempting to Access a Protected Computer Without Authorization, in violation of 18 U.S.C. § 1030(a)(2)(C). The essential elements of a violation of 18 U.S.C. § 1030(a)(2)(C) and 1030(b)[2] are:

(1) One, the defendant David Shen intentionally attempted to accessed a computer without authorization and

(2) Two, the defendant attempted to obtain information from any protected computer.

If the jury finds these two elements have been proven beyond a reasonable doubt, in order to trigger the felony provisions of 18 U.S.C. § 1030(c)(2)(B)(i) & (iii), the jury must then unanimously find that the answer to one of the following three questions is "yes":

(1) Did the defendant act for purposes of commercial advantage or private financial gain?

(2) Did the defendant obtain information that had a value exceeding $5,000.00?

If the jury finds that the answer to either of these two questions is "yes," then the felony provisions of 18 U.S.C. § 1030(c)(2)(B)(i) & (iii) have been satisfied.

Regarding the factor identified in § 1030(c)(2)(B)(ii) – that the defendant acted in furtherance of a crime or tort – although the government alleged that factor in the indictment in charging the provisions of the statute in the conjunctive, it does not intend to proceed on it as a theory at trial.

> this fact neither renders the indictment bad for duplicity nor precludes a conviction if only one of the several allegations linked in the conjunctive in the indictment is proven.

United States v. McCann, 465 F.2d 147, 162 (5th Cir.), *cert. denied*, 412 U.S. 927 (1972); *see United States v. Mohr*, 728 F.2d 1132, 1135 (8th Cir.), cert. denied, 469 U.S. 843 (1984)("Where a statute specifies two or more ways in which an offense may be committed, however, all may be alleged in the conjunctive in one count of the indictment, and proof of any one of the acts conjunctively charged may establish guilt.").

2 18 U.S.C. § 1030(b) provides that "Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section."

C. Definitions

(1) Computer

The Eighth Circuit pattern instructions for offenses in violation of 18 U.S.C. § 1030(a)(2)(C) provide that, "the term 'computer,' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device." Model Crim. Jury Instr. 8th Cir. 6.18.1030I. The government anticipates that its proof at trial will establish that the Albourne and Burgiss servers constitute a high speed data processing device performing logical or storage functions.

(2) Protected Computer

The phrase "protected computer," as used in the statute and in the pattern Eighth Circuit instructions, refers to a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." Model Crim. Jury Instr. 8th Cir. 6.18.1030I.

(3) "Without authorization"

Although the indictment alleges two alternative theories in Count 1 – both that the defendant exceeded his previously given authorized access and that he acted without authorization – the government intends to proceed at trial on the theory that the defendant accessed the Albourne and Burgiss servers without authorization, given that his employment, and thus, his means of lawful access to those servers, had been terminated. As the Magistrate's Report and

Recommendation concerning the motion to dismiss recognizes, "[t]he indictment reflects that Shen was given access to Service Provider A in connection with his employment and that he accessed Service Provider A after he had resigned. There is significant authority that such access is unauthorized under § 1030(a)(2)(C). *See*, *e.g.*, *United States v. Steele*, No. 13-4567, 2014 WL 7331679 (4th Cir. Dec. 24, 2014); *cf. United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011)." Doc. No. 36 at 3.

The Eighth Circuit instructions provide that although "'without authorization' is not defined in section 1030," that term "is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever." (citing *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted)). Model Crim. Jury Instr. 8th Cir. 6.18.1030B n. 2 (2014).

D. Federal Jurisdiction

The jurisdictional basis for prosecution of unauthorized access of a protected computer derives from the use of that computer in interstate or foreign commerce or communication. See 18 U.S.C. § 1030(e)(2)(b) (defining a "protected computer" as a "computer . . . which is used in or affecting interstate or foreign commerce or communication."). The protected computers in question here consist of the Albourne and Burgiss servers. The government anticipates that the parties will reach an evidentiary stipulation as to the use of those servers in interstate commerce and communication. In the event that the parties are unable to agree to a stipulation, the government anticipates that witnesses employed by Albourne and Burgiss will establish that the servers transmit records across state lines and provide services to people throughout the United States, and thus, are used in interstate and foreign commerce.

E. Elements of Wire Fraud – 18 U.S.C. § 1343

Count Three of the indictment charges the defendant with intentionally executing a scheme to defraud by means of transmitting wire communications in interstate commerce. The elements of this offense are as follows:

(1) *One*, the defendant voluntarily and intentionally devised a scheme to defraud and to obtain money or property by means of material false representations or promises;
(2) *Two*, the defendant did so with the intent to defraud; and
(3) *Three*, in advancing, furthering, or carrying out the scheme, the defendant transmitted or caused to be transmitted any writing, signal, or sound by means of a wire, radio, or television communication in interstate commerce, to wit, a telephone call from the defendant to a representative of the Burgiss service.

Model Crim. Jury Instr. 8th Cir. 6.18.1341 (2014)(modified to reflect wire, rather than mail, fraud).

F. Definitions

(1) Scheme to Defraud

The phrase "scheme to defraud" includes any plan or course of action intended to deceive or cheat another out of money or by employing material falsehoods, concealing material facts and omitting material facts. It also means the obtaining of money or property from another by means of material false representations or promises. A scheme to defraud need not be fraudulent on its face but must include some sort of fraudulent misrepresentation or promise reasonably calculated to deceive a reasonable person. Model Crim. Jury Instr. 8th Cir. 6.18.1341 (2014).

(2) Material Misrepresentations

A statement or representation is "false" when it is untrue when made or effectively conceals or omits a material fact.

A fact or representation is "material" if it has a natural tendency to influence, or is capable of influencing, the decision of a reasonable person in deciding whether to engage or not to engage in a particular transaction. However, whether a face or representation is "material" does not depend

on whether the person was actually deceived. With respect to false statements, the defendant must have known the statement was untrue when made or have made the statement with reckless indifference to its truth or falsity. Model Crim. Jury Instr. 8th Cir. 6.18.1341 (2014).

(3) Intent to Defraud

To act with "intent to defraud" means to act knowingly and with the intent to deceive someone for the purpose of causing some financial loss or loss of property to another or bringing about some financial gain to oneself or another to the detriment of a third party.

The term "property rights," as used in the wire fraud statute, includes intangible as well as tangible property rights. It includes any property right which has a value—not necessarily a monetary value—to the owner of the property right. For example, a scheme to deprive a company of the exclusive use of confidential business information obtained by the employees would be a scheme to deprive the company of intangible property rights. Model Crim. Jury Instr. 8th Cir. 6.18.1341 (2014).

IV. Evidentiary Issues

A. Intrinsic and relevant evidence Fed Rule Evid. 401

In the present case, the government intends to introduce evidence through representatives from the Albourne and Burgiss services that the defendant downloaded dozens of documents from both services after he was no longer employed by Washington University. The government will limit the evidence of the defendant's additional downloads, beyond the Risk Report, to the indexes created by Albourne and Burgiss that identify the source databases, and in the case of Albourne, the originating IP address.

The government's position is that this evidence is intrinsic evidence of the charged offenses – accessing and attempting to access protected computers without authorization and a

scheme to defraud by means of material misrepresentations. Intrinsic evidence is that which "relate[s] to an integral part of the immediate context of the crime charged." *United States v. LeCompte*, 108 F.3d 948, 952 (8th Cir. 1997) (citing *United States v. Waloke*, 962 F.2d 824, 828 (8th Cir. 1992)); *United States v. Bass*, 794 F.2d 1305, 1312 (8th Cir.) *cert. denied*, 479 U.S. 869 (1986).

Although the indictment identifies one document specifically in Count 1 (the Risk Report) as having been impermissibly downloaded from the Albourne service, Counts 1 describes the defendant's offense conduct as having "used his person computer to access without authorization . . . a computer system associated with Service Provider A." Counts 2 and 3 describe the defendant's attempt to access the entirety of the Burgiss databases without authorization in an attempt to obtain information to which he was not legally entitled. The Eighth Circuit has repeatedly recognized that "[w]here evidence of other crimes is so blended or connected, with the ones on trial as that proof of one incidentally involves the others; or explains the circumstances; or tends logically to prove an element of the crime charged, it is admissible as an integral part of the immediate context of the crime charged." *United States v. Luna*, 94 F.3d 1156, 1162 (8th Cir. 1996); *United States v. Derring*, 592 F.2d 1003, 1007 (8th Cir. 1979); *United States v. Mandacina*, 45 F.3d 1177, 1188 (8th Cir. 1995).

The evidence described above provides the background and context for the crime charged in the indictment. Such evidence helps "to complete the story of the crime on trial by proving its immediate context or the 'res gestae'." *United States v. Carter*, 549 F.2d 77, 78 (8th Cir. 1977). Similarly, "[a] jury is entitled to know the circumstances and background of a criminal charge. It cannot be expected to make its decision in a void - without knowledge of the time, place, and circumstances of the acts which form the basis of the charge." *United States v. Moore*, 735 F.2d

289, 292 (8th Cir. 1984).

The Government's position is that no analysis under Federal Rule of Evidence 404(b) is necessary. Evidence such as that detailed above is intrinsic when the evidence of the other acts and the evidence of the crime charged are "inextricably intertwined," when both acts are part of a single criminal episode, or when the other acts were necessary preliminaries to the crime charged. *United States v. Williams*, 900 F.2d 823, 825 (5th Cir. 1990); *United States v. Stovall*, 825 F.2d 817 (5th Cir. 1987); *United States v. Roylance*, 690 F.2d 164 (10th Cir. 1982). Also, evidence is intrinsic when the acts complete the story of the crime on trial. *United States v. Senffner*, 280 F.3d 755, 764 (7th Cir. 2002), *cert. denied*, 536 U.S. 934 (2002); or evidence that explains the circumstances of the case. *United States v. Holt*, 460 F.3d 934 (7th Cir. 2006).

In *United States v. Kirkham*, 129 Fed.Appx. 61, 65, 2005 WL 827119, *2 (5th Cir. 2005), the defendants were charged with executing a scheme or artifice to defraud a health care benefits program in violation of 18 U.S.C. § 1347. The *Kirkahm* indictment listed 13 particular transactions executed or attempted to be executed in perpetrating the scheme to defraud. *Id.* at 64-65. On appeal, the *Kirkham* defendants challenged the trial court's admission of "evidence of fraudulent transactions that were not specified in the indictment" as impermissible per Fed.R.Evid. 404(b). *Id.* at 73. The defendants "contend[ed] that these transactions constitute evidence of extrinsic bad acts, requiring the trial court to weigh the probative value of the evidence against unfair prejudice to the defendants as a result of its admission. Defendants argue[d] further that, as the government did not disclose its intention to introduce this evidence at trial pursuant to defendants' 404(b) motion to disclose, they did not receive fair notice that such evidence would be introduced against them at trial." *Id.*

The Court of Appeals rejected the defendants' argument, holding that "[i]f the existence of

a scheme to defraud is an element of the offense, then acts and transactions constituting a part of that continuing offense are admissible as proof of the criminal enterprise. Evidence of an uncharged offense arising out of a scheme or artifice to defraud is not 'extrinsic' within the meaning of 404(b) and thus not excludable on this ground. The prosecution may offer evidence of any surrounding circumstances that are relevant to prove intent or motive with respect to the fraudulent scheme." *Id.* (emphasis added) (citing at n.48 *United States v. Stouffer*, 986 F.2d 916, 926 (5th Cir.1993). As in *Kirkham*, here, evidence of the defendant's repeated unauthorized access of the Albourne and Burgiss databases is proof of the existence of the defendant's scheme to defraud, as charged in Count 3 of the indictment. It is also evidence that the defendant, as charged in Count 1, "used his personal computer to access without authorization, a computer system associated with Service Provider A." The fact that the indictment identifies one particular document out of the hundreds of documents downloaded by the defendant from the Albourne (Service Provider A) database should not artificially restrict the scope of the government's proof to that single document. The downloading of that document was made possible by the defendant's repeated unauthorized access of the Albourne database, and thus, evidence of those repeated unauthorized accesses does not constitute extrinsic evidence, but rather, intrinsic evidence of the offense charged in Count 1.

Regarding Counts 2 and 3, the government's evidence will establish that through an oversight, the defendant's access to only 3 out of the 4 Burgiss databases was terminated. The index of documents downloaded by the defendant from the Burgiss database will reflect that the defendant repeatedly accessed the one database to which he still had access. The government's proof at trial will establish that the defendant contacted Burgiss in order to restore his access to all four of the databases. Evidence that the defendant repeatedly accessed the only Burgiss database

for his password had not been locked provides vitally important context for the conduct charged in Counts 2 and 3 – namely, that the defendant contacted Burgiss, misrepresenting himself as still employed by WU, and then sought to unlock his password to the 3 databases to which his access had been terminated. As with the evidence of the defendant's access of the Albourne database, the log of the defendant's access of the Burgiss database is intrinsic to the offenses charged in Counts 2 and 3, and thus, should be admitted as relevant.

B. Evidence of the Supposed Misdeeds of the Defendant's Employers Should Be Excluded as Irrelevant and Not Probative of Truthfulness.

During the defendant's interview with law enforcement agents, the defendant repeatedly indicated that he had anonymously emailed the documents he had pulled from his supervisor's file folders because he felt that his supervisor, Brian Wentworth, was proposing ideas to the WU Board of Directors that were "too risky" and that the Board was thus "receiving an incomplete picture of the issue." The government now seeks to preclude the defendant, either during cross-examination of the government's witnesses, specifically, Kim Walker, an employee of WU, or during the defendant's case-in-chief, from asserting that his access of the Albourne or Burgiss databases following his termination was in some way justified because he felt that his supervisor had failed to apprise WU of investment risks. Such evidence has no relevance to the charged conduct, and would essentially amount to a justification or coercion defense, which is not available to the defendant in the present case.

The Eighth Circuit pattern instructions provide that the defendant carries the burden of proof for a justification defense, and that the defendant must establish that "[i]f the defendant committed the crime of (describe offense) only because he reasonably feared that immediate, serious bodily harm would be inflicted upon him, if he did not commit the crime, and if the

defendant had no reasonable opportunity to avoid that harm, then he was coerced." Model Crim. Jury Instr. 8th Cir. 9.02 (2014). "In general, to establish a justification defense a defendant must show that: 1) he was under an unlawful and present, imminent, and impending threat of such a nature as to induce a well-grounded apprehension of death or serious bodily injury; 2) that he had not recklessly or negligently placed himself in a situation in which it was probable that he would be forced to commit a criminal act; 3) that he had no reasonable, legal alternative to violating the law; and 4) that a direct causal relationship may be reasonably anticipated between the commission of the criminal act and the avoidance of the threatened harm." *United States v. Lomax*, 87 F.3d 959, 961 (8th Cir. 1996). There is no evidence here that the defendant felt any unlawful and present threat of death or bodily injury, and thus, the coercion or duress argument should not be available to the defendant as a method of proof.

Further, any cross-examination on this issue would constitute improper impeachment within the meaning of Fed.R.Evid. 608(b), which provides that "the court may, on cross-examination, allow [specific instances of a witness's conduct] to be inquired into if they are probative of the character for truthfulness or untruthfulness of: (1) the witness; or (2) another witness whose character the witness being cross-examined has testified about." The government does not intend to call Brian Wentworth as a witness, nor does it intend to elicit testimony from Kim Walker concerning Brian Wentworth's character for truthfulness. Because any testimony concerning Wentworth's supposed failure to adequately apprise the Board of Directors of investment risks falls outside the purview of permissible impeachment, the government respectfully requests that the defense be precluded from any questioning on that issue.

V. Logistical Issues

A. Summary and Demonstrative Exhibits

The Government intends to use a summary chart outlining the defendant's access of the Albourne database to download the Risk Report, the IP address used to access that database, and the corresponding IP address on the defendant's computer. This chart will summarize records from Charter communications reflecting the defendant's IP address and records from Albourne showing the IP address from which the downloaded risk report was accessed. It has long been the rule that charts of the sort involved here may be exhibited to the jury during the trial in the discretion of the trial court in order that they "may guide and assist the jury in understanding and judging the factual controversy." *United States v. Downen*, 496 F.2d 314, 321 (10th Cir. 1974). *See also United States v. Johnson*, 319 U.S. 503, 519 (1942); *United States v. Orlowski*, 808 F.2d 1283, 1289 (8th Cir. 1986); *United States v. Nelson*, 735 F.2d 1070, 1072 (8th Cir. 1984); *United States v. Katz*, 705 F.2d 1237 (10th Cir. 1983); *United States v. Behrens*, 689 F.2d 14 (10th Cir.), *cert. denied*, 103 S. Ct. 573 (1982); *United States v. King*, 616 F.2d 1034, 1041 (8th Cir.), *cert. denied*, 446 U.S. 969 (1980); *United States v. Skalicky*, 615 F.2d 1117, 1120-21 (5th Cir.), *cert. denied*, 449 U.S. 832 (1980); *United States v. Foshee*, 606 F.2d 111, 113 (5th Cir. 1979), *cert. denied*, 444 U.S. 1082 (1980); *United States v. Scales*, 594 F.2d 558, 561-64 (6th Cir.), *cert. denied*, 441 U.S. 946 (1979); *United States v. Normile*, 587 F.2d 784, 787 (5th Cir. 1979); *United States v. Ellenbogen*, 365 F.2d 982, 988 (2d Cir. 1966), *cert. denied*, 386 U.S. 923 (1967). *See*, generally, Fed. R. Evid.1006.

District courts have routinely allowed the government to introduce charts and summaries based on the evidence, pursuant to Federal Rule of Evidence 1006. *See United States v. Johnson*, 319 U.S. 503, 519 (1943); *United States v. Bishop*, 264 F.3d 535, 548 (5th Cir. 2001)548 (permitting the use of charts and summaries in a tax trial); *United States v. Gardner*, 611 F.2d 770, 776 (9th Cir. 1980); *see also* Fed. R. Evid. 1006 (permitting the use of charts and summaries of

voluminous records, even when the underlying records are not produced in court). Summaries prepared by a government witness need not contain the defendant's anticipated evidence. *See Myers v. United States*, 356 F.2d 469, 470 (5th Cir. 1966); *Barsky v. United States*, 339 F.2d 180, 181 (9th Cir. 1964). Furthermore, copies of the summaries may be circulated to the jury during the testimony concerning them. *See Barsky*, 339 F.2d at 181. The summaries may also be used by the jury during deliberations. *See Bishop*, 264 F.3d at 547; *United States v. Possick*, 849 F.2d 332, 339 (8th Cir. 1988).

The Eighth Circuit, in *United States v. Smallwood*, 443 F.2d 535 (8th Cir.), *cert. denied*, 404 U.S. 853 (1971), allowed the admission of charts that summarized other exhibits. The court stated, as follows:

> The court room use of summaries of business records, particularly where the actual records are voluminous and complex, is not only proper but advisable. (Citations omitted) Evidential use of such summaries rests within the sound discretion of the trial judge, whose action in allowing their use may not be disturbed by the appellate court except for an abuse of discretion. Id. at 540. See also King, 616 F.2d at 1034.

Computer printouts which summarize voluminous evidence are also permissible under Rule 1006. *City of Phoenix v. Com/Systems, Inc.*, 706 F.2d 1033 (9th Cir. 1983); *United States v. Johnson*, 594 F.2d 1253, 1254-57 (9th Cir.), *cert. denied*, 444 U.S. 464 (1979); *United States v. Smyth*, 556 F.2d 1179 (5th Cir. 1977).

In *Smallwood*, the summaries in issue were based on materials already in evidence or that were being admitted. The same will be true here. In *Smallwood*, the court cited with favor a prior Eighth Circuit case which reasoned, "[e]xhibits which may facilitate understanding of complex factual issues are to be encouraged for court room use." *Boston Securities, Inc. v. United Bonding Insurance Co.*, 441 F.2d 1302, 1303 (8th Cir. 1971). *See also United States v. Brickey*, 426 F.2d 680, 686-87 (8th Cir.), *cert. denied*, 400 U.S. 828 (1970); *Ping v. United States*, 407 F.2d

157, 159-160 (8th Cir. 1969) (summaries of checking accounts records in criminal tax case). Thus, it is clearly within the discretion of the trial court to allow the use of charts at trial where they would be of assistance to the jury, subject to the appropriate limiting instructions, and such discretion will be subject to review only upon a clear showing of abuse and resulting prejudice to the opposing party. *Smallwood*, 443 F.2d at 540; *Brickey*, 426 F.2d at 686-87; *King*, 616 F.2d at 1034.

The government intends to admit this summary chart through the testimony of SA Ashley Frazer, the case agent. Because a summary witness's testimony is based on evidence admitted at trial, his or her presence in the courtroom throughout trial is permitted, even when other witnesses are sequestered pursuant to Federal Rule of Evidence 615. *See United States v. Strauss*, 473 F.2d 1262, 1263 (3d Cir. 1973); *United States v. Mohney*, 949 F.2d 1397, 1404 (6th Cir. 1991); *United States v. Bertoli*, 854 F. Supp. 975, 1037 (D.N.J. 1994). The government therefore requests that SA Frazer be permitted to remain in the courtroom throughout the trial as a potential summary witness.

The use of charts in the opening statement and closing argument is governed by the same principles that apply to the use of charts at trial. *See United States v. Churchill*, 483 F.2d 168 (1st Cir. 1973); *United States v. Rubino*, 431 F.2d 284 (6th Cir. 1970). As described above, the charts will help the jury picture the structure of the transactions at issue and the relationships of the defendants, witnesses and entities involved, thereby effectuating the recognized goal of an opening statement -- "to give the broad outlines of the case to enable the jury to comprehend it," *Virgin Islands v. Turner*, 409 F.2d 102, 103 (3d Cir. 1969), and "to make it easier for the jurors to understand what is to follow, and to relate parts of the evidence and testimony to the whole." *United States v. Dinitz*, 424 U.S. 600 (1976) (Burger, C.J., concurring).

B. Expert Testimony

At trial, the Government plans to introduce expert opinion testimony from Det. Wilds regarding the forensic examination of the defendant's computer, the external thumb drive, and peripherals. Prior to eliciting the opinion testimony, the Government will qualify any witness as experts on the basis of the witnesses participation in numerous computer forensic examinations education. Under the prevailing case law, the Government's anticipated opinion testimony is clearly admissible.

Under Federal Rule of Evidence 702, a qualified witness may testify as an expert, "(i)f scientific, technical or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702. The expert's testimony is still admissible even if it "embraces an ultimate issue to be decided by the trier of fact." Fed. R. Evid. 704. However, no expert testimony may be admitted as to whether the defendant had the requisite mental state constituting an element of the crime. *Id.* Admission of expert testimony or lay opinion testimony is a matter within the broad discretion of the trial judge that will not be disturbed absent clear abuse. *United States v. Hughes*, 15 F.3rd 798, 800 (8th Cir. 1994). The government has provided to the defense notice of its intent to call Det. Wilds as an expert, in addition to a copy of Det. Wilds' forensic report and CV.

Federal courts have routinely permitted law enforcement agents to give expert testimony in a variety of areas. *See United States v. Riccobene*, 709 F.2d 214 (3d Cir.) (FBI agent testimony defining terms "LaCosa Nostra," "capi," "consigliere"); United States v. Carson, 702 F.2d 351 (2d Cir.), cert. denied, 103 S.Ct. 2456-57 (1983) (DEA agent testimony that defendant's furtive activity appeared to be drug sales); *United States v. Scavo*, 593 F.2d 837 (8th Cir. 1979) (FBI agent testimony regarding nature of gambling operations and gambling terminology); *United*

States v. Masson, 582 F.2d 961 (5th Cir. 1978) (expert testimony regarding meaning of terminology used in bookmaking operation); *United States v. Barletta*, 565 F.2d 985 (8th Cir. 1977), cert. denied, 430 U.S. 905 (FBI agent testimony about structure of bookmaking operations); *United States v. Jackson*, 425 F.2d 574 (D.C. Cir. 1970) (expert testimony concerning the modus operandi of pickpockets).

VI. Conclusion

The foregoing are the issues that the Government expects to arise in the trial of this matter.

Respectfully submitted,

RICHARD G. CALLAHAN
United States Attorney

s/ Gwendolyn E. Carroll
Gwendolyn E. Carroll – 4657003NY
Assistant United States Attorney